CLAIMS

What is claimed is:

1. A user authentication method that authenticates a user based on a password input by the user and the user's biometrics information, the user authentication method comprising:

determining whether a password has been input;

setting a first threshold value if the input password matches with a registered password and setting a second threshold value if the input password does not match with the registered password; and

determining whether to authenticate the user based on a comparison of the user's biometrics information with registered biometrics information and the first or second threshold value.

2. The user authentication method of claim 1, wherein the first threshold value is set so that a false rejection rate (FRR) is reduced and the second threshold value is set so that a false acceptance rate (FAR) is reduced.

3. The user authentication method of claim 1, further comprising:

storing a password input history; and

determining whether there has been an intrusion, by referring to the password input history if the user is not authenticated.

4. The user authentication method of claim 3, further comprising:

storing an intruder's biometrics information upon determining that there has been an intrusion,

wherein the determining whether there has been an intrusion, comprises authenticating the user based on a result of comparing the user's biometrics information with the intruder's biometrics information.

5. The user authentication method of claim 1, further comprising:

storing a password input history; and

varying the first and second threshold values based on the password input history if the user is not authenticated.

6. The user authentication method of claim 5, wherein the varying the first and second threshold values, comprises varying the first and second threshold values so as to enhance a level of security if a wrong password is input at least n times.

7. The user authentication method of claim 6, wherein the varying the first and second threshold values, comprises restoring the varied first and second threshold values if a correct password is input at least m times after the first and second threshold values are varied so as to enhance the level of security.

8. The user authentication method of claim 1, further comprising:

adding/updating an authentication key if the user is authenticated.

9. The user authentication method of claim 8, wherein the adding/updating the authentication key, comprises adding/updating the authentication key if the input password matches with the registered password and the user is authenticated by a biometrics unit.

10. The user authentication method of claim 8, wherein the adding/updating the authentication key, comprises adding/updating the authentication key if the user is authenticated by the biometrics unit and the extent to which the input password matches with the registered password is larger than a predetermined third threshold value.

11. A user authentication apparatus that authenticates a user based on a password input by the user and the user's biometrics information, the user authentication apparatus comprising:

a password input unit which determines whether a password has been input;

a storage unit which stores a registered password and registered biometrics information;

a threshold value setting unit which sets a first threshold value if the input password matches with a registered password and sets a second threshold value if the input password does not match with the registered password; and a biometrics unit which obtains biometrics information from the user outside, determines how much the obtained biometrics information matches with the registered biometrics information, and authenticates a user if the extent to which the obtained biometrics information matches with the registered biometrics information is larger than the first or second threshold value.

12. The user authentication apparatus of claim 11, wherein the first threshold value is set so that a false rejection rate (FRR) is reduced and the second threshold value is set so that a false acceptance rate (FAR) is reduced.

13. The user authentication apparatus of claim 11, wherein the storage unit stores a password input history, and the biometrics unit determines whether there has been an intrusion by referring to the password input history stored in the storage unit if the user is not authenticated.

14. The user authentication apparatus of claim 13, wherein the storage unit stores an intruder's biometrics information if determined that there has been an intrusion, and the biometrics unit authenticates the user based on a result of comparing the obtained biometrics information with the intruder's biometrics information.

15. The user authentication apparatus of claim 11, wherein the storage unit stores a password input history, and the threshold value setting unit varies the first and second threshold values based on the password input history if the user is not authenticated.

16. The user authentication apparatus of claim 15, wherein the threshold value setting unit varies the first and second threshold values so that a level of security is enhanced, if an incorrect password is input n times or more.

17. The user authentication apparatus of claim 16, wherein the threshold value setting unit restores the varied first and second threshold values if a correct password is input m times or more.

18. The user authentication apparatus of claim 11, wherein an authentication key is added or updated if the user is authenticated.

19. The user authentication apparatus of claim 18, wherein the authentication key is added or updated if the input password matches with the registered password and the user is authenticated by the biometrics unit.

20. The user authentication apparatus of claim 18, wherein the authentication key is added or updated if the user is authenticated by the biometrics unit and the extent to which the obtained biometrics information matches with the registered biometrics information is larger than a predetermined third threshold value.

21. The user authentication apparatus of claim 11, further comprising:

a counter which counts the number of times an incorrect password is input and outputs a result of the counting,

wherein the threshold value setting unit varies the first or second threshold value depending on the result of the counting.

22. The user authentication apparatus of claim 11, further comprising:

a counter which counts the number of times an incorrect password is input and outputs a result of the counting,

wherein the storage unit stores the obtained biometrics information output from the biometrics unit depending on the result of the counting.

23. A computer-readable recording medium on which a program enabling the user authentication method of claim 1 is recorded.

24. A user authentication method, comprising:

adjusting a threshold level of a biometrics device which reads a user's biometric information based on a password input by a user, wherein the threshold level is broadened when the user inputs a valid password to increase the possibility of the user being authenticated by the biometrics device, and the threshold level is narrowed when the user inputs an invalid password to decrease the possibility of the user being authenticated by the biometrics device.

25. The method of claim 24, further comprising:

comparing the user input password with a predetermined password, wherein when the user input password is valid, the user input password matches the predetermined password, a first threshold level which reduces a false rejection rate is set, and when the user input password is invalid, the user input password does not match the predetermined password, a second threshold level which reduces a false acceptance rate is set.

26. The method of claim 24, wherein the threshold level is adjusted to incrementally reduce the possibility of the user being authenticated by the biometrics device as a number of invalid password entries by the user increases.

27. The method of claim 26, further comprising:

storing the user's biometric information as an intruder biometric entry when the number of invalid password entries by the user equals a predetermined number.

28. The method of claim 27, further comprising:

comparing a subsequent user's biometric information with the intruder biometric entry, wherein when the subsequent user's biometric information matches the intruder biometric entry based on the threshold level set, the subsequent user is blocked from being authenticated.

29. The method of claim 26, further comprising:

storing the password input by the user as a password history; and

storing the user's biometric information as an intruder biometric entry based on the password history.

30. The method of claim 29, further comprising:

comparing a subsequent user's biometric information with the intruder biometric entry, wherein when the subsequent user's biometric information matches the intruder biometric entry based on the threshold level set, the subsequent user is blocked from being authenticated.

31. The method of claim 24, further comprising:

storing a biometric authentication key which corresponds to an authorized user's biometric information; and

updating the authentication key when the password is valid.

32. The method of claim 31, wherein the updating the authentication key occurs only when the password is valid and the level which the user's biometric information matches the authorized user's biometric information exceeds an updating authentication threshold.

33. A user authentication method, comprising:

authenticating a user by varying a threshold value of a biometrics device depending on whether a password input by the user matches a registered password.

34. The method of claim 33, wherein the threshold value comprises a first threshold value when the password input by the user matches the registered password and a second threshold value when the password input by the user does not match the registered password.

35. The method of claim 34, further comprising:

varying the first and second threshold values to enhance a level of security when an incorrect password has been entered a predetermined number of times.